

## The Validity of Online Agreements and The Power of Digital Evidence in Treaty Law in Indonesia

**Mochamad Fachrurozi\*, Harmono**

Universitas Swadaya Gunung Jati, Indonesia

Email: mochfachrurozi721@gmail.com\*, harmono@ugj.ac.id

---

### Keywords:

Online Agreements;  
Digital Proof; Validity

---

### Abstract

The shift from conventional transactional paradigms to the digital realm creates juridical ambiguity regarding the requirements for the validity of contracts and the admissibility of evidence in civil disputes. This normative legal research aims to analyze the synchronization of Article 1320 of the Civil Code with the ITE Law, as well as evaluate the evidentiary weight of electronic evidence from the perspective of civil procedure law in Indonesia. Using statutory and conceptual approaches, the study finds that electronic contracts remain subject to the classical doctrine of the Civil Code, where the absence of an age verification system on digital platforms has the potential to render agreements voidable. Furthermore, the unilateral imposition of standard clauses frequently undermines the principle of freedom of contract and prejudices the position of consumers. In terms of evidence, the legitimacy of digital evidence continues to be constrained by the absence of adequate forensic operational procedure standards, giving rise to disparities in judicial decisions. The study concludes that the renewal of legal norms has not been accompanied by corresponding technical readiness within the judiciary. It is therefore recommended that a real-time population data system be integrated for the verification of legal subjects, and that a Supreme Court Regulation be issued specifically governing the guidelines for the examination of electronic evidence, in order to ensure legal certainty and consumer protection in cyberspace.

---

### INTRODUCTION

The development of information and communication technology is driving a paradigm shift in business, social, and cultural interactions, producing new transaction mechanisms commonly known as online agreements or electronic contracts (e-contracts). This technology has rapidly influenced the economic system in Indonesia, where online agreements are concluded between producers and consumers (Usman, 2020). The use of electronic systems in economic activity is now widespread, offering convenience, speed, and efficiency. Fundamentally, the Indonesian civil law system recognizes the applicability of online agreements, as this recognition constitutes the primary basis from which rights and obligations arise for parties entering into such agreements.

In response to these developments, the Indonesian government enacted Law Number 11 of 2008 concerning Information and Electronic Transactions (the ITE Law), subsequently amended by Law Number 1 of 2024. This regulation explicitly provides legal recognition of electronic information and electronic documents as valid evidence, thereby establishing legal certainty that online agreements are valid provided they satisfy the conditions set out in Article 1320 of the Civil Code (Kakisina et al., 2023). In line with technological developments, an agreement or contract may now be concluded without the parties meeting in person, carrying the same legal force as a conventional written agreement (Bernstein, 2015; Savelyev, 2017).

Despite this regulatory framework, the application of online agreements continues to raise significant juridical problems, particularly concerning synchronization with the conditions for the validity of agreements. Issues relating to legal capacity and free will are especially pronounced in online agreements, which are largely automated and frequently take the form of standard contracts. Many minors, who lack the legal capacity to enter into electronic transactions, continue to access and use them. This creates difficulties in verifying that parties to an online agreement are legally competent, giving rise to the potential for future disputes regarding the validity of such agreements.

With respect to the proof of digital evidence within the contractual legal system, the recognition of electronic evidence derives normative legitimacy from the ITE Law and its amendments. However, this formal recognition does not fully guarantee uniformity of practice, as the technical and juridical challenges in assessing the validity and evidentiary weight of digital evidence remain complex. Divergent interpretations of the authenticity, integrity, and relevance of digital evidence raise serious questions about its probative strength (Bachsin et al., 2025). Although the use of electronic evidence has the potential to facilitate a more transparent and accountable judiciary, an in-depth analysis is needed to establish juridical standards that would allow digital evidence to be accepted as conclusive proof in court proceedings.

Several studies have examined the validity of online agreements and digital evidence in Indonesia. Research by Usman (2020) and Kakisina et al. (2023) analyzed the legal recognition of electronic contracts under the ITE Law but did not thoroughly explore their synchronization with the subjective validity requirements of the Civil Code. Studies by Pohan et al. (2023) and Debora et al. (2024) highlighted the issue of standard clauses in electronic contracts, yet their analyses remained descriptive without offering concrete reform proposals. With regard to digital evidence, Bachsin et al. (2025) and Pradipa & Ganesha (2025) identified the absence of uniform standards for electronic evidence admissibility but did not provide an integrated solution linking contract validity and evidentiary strength. Overall, prior research tends to be fragmented, addressing either contract validity or digital evidence in isolation rather than within a coherent legal framework.

These practice gaps give rise to legal uncertainty regarding the validity of online agreements and the evidentiary weight of digital evidence. Although online agreements are widely used, differences in interpretation regarding their validity and the probative force of digital evidence persist in practice, creating conditions for legal uncertainty. This research is therefore important to analyze through the lens of contract law doctrine. Its novelty lies in integrating contract validity and digital evidence analysis within a single framework, identifying specific judicial obstacles such as the absence of digital forensic standard operating procedures, and formulating policy recommendations including a real-time population verification system and a Supreme Court Regulation on digital evidence standards.

The objectives of this research are to analyze the synchronization between Article 1320 of the Civil Code and the ITE Law regarding the validity of online agreements, to evaluate the evidentiary strength of electronic evidence from the perspective of civil procedure law in Indonesia, and to formulate legal reform recommendations to provide certainty and consumer protection in cyberspace. The benefits are both theoretical and practical. Theoretically, the research enriches the literature on contract and evidence law by harmonizing conventional legal

doctrines with the digital ecosystem and contributes to legal theory development in developing countries. Practically, it provides input for policymakers — including the Kementerian Komunikasi dan Informatika, the Supreme Court, and legislators — in addressing age verification gaps, standard clause abuses, and the absence of digital forensic standards, while also serving as a reference for judges, legal practitioners, and researchers.

## **METHOD**

In examining the legal issues surrounding the validity of online agreements and their evidentiary strength, the authors employ a combination of integratively structured approaches to obtain comprehensive analytical results. The research applies a legislative approach in conjunction with a conceptual approach to examine the relationship between regulations and developing legal doctrines. The legislative approach is carried out by tracing the internal consistency of the provisions of the Civil Code (*Kitab Undang-Undang Hukum Perdata/KUHPerdata*) against the *lex specialis* provisions of Law Number 1 of 2024 concerning Information and Electronic Transactions. The conceptual approach serves as a complementary tool for filling legal gaps by reference to fundamental legal principles such as the principle of functional equivalence. Through this combination, the research aims to construct a conceptual framework capable of explaining how electronic information can satisfy both the objective and subjective requirements of a valid agreement and carry sufficient evidentiary weight before a court.

This research employs a normative juridical methodology, which involves the collection and analysis of legal materials in accordance with the selected research approach (Sutrisno et al., 2021). According to Soerjono Soekanto, normative juridical research — often referred to as library law research — is legal research conducted exclusively through the examination of secondary data or literary materials (Soerjono & Sri, 2007). This methodological choice is grounded in the nature of the problems examined: this study does not seek to assess the sociological effectiveness of the law in practice but focuses instead on the analysis of positive legal norms, legal principles, and the vertical and horizontal synchronization of laws and regulations. From a normative perspective, law is treated as a logical and consistent system of rules, and the study centers on identifying the relationship between the validity requirements of conventional agreements and the dynamics of electronic transactions. The authors treat legal materials as primary data, analyzed through legal logic to identify normative gaps and regulatory inconsistencies in the current practice of online agreements.

This study draws primarily on deductive data sources obtained through literature research, with legal materials classified hierarchically. The analysis is conducted in a descriptive-analytical manner. According to Soerjono Soekanto, descriptive-analytical research aims to provide a detailed, systematic, and comprehensive account of all matters pertaining to the problem under study (Soerjono, 1986). This analysis employs legal interpretation techniques — both grammatical and systematic — to synthesize fragmented regulatory provisions into coherent juridical solutions. The analysis evaluates the conformity between the objective and subjective requirements of agreements within the digital ecosystem in order to assess the validity of electronic contracts. It further aims to provide recommendations regarding the parameters by which judges should assess the authenticity of digital evidence, with a view to promoting uniformity of decisions in digital civil cases.

## RESULTS AND DISCUSSION

### H.1. Dynamics and Juridical Construction of the Validity of Online Agreements in the National Civil Law Structure

The rapid development of information and communication technology has deconstructed the traditional order in civil transactions, compelling a paradigm shift from conventional dealings that rely on physical mediums such as paper to an intangible digital ecosystem. In examining the validity of online agreements or electronic contracts (e-contracts), the analytical starting point cannot be separated from the ontological foundation of contract law as set out in Book III of the Civil Code (Kitab Undang-Undang Hukum Perdata/KUHPerdata). Fundamentally, the Indonesian civil law system rests on the principle of freedom of contract and the principle of consensualism, which affirm that a legal obligation arises at the moment of agreement or meeting of wills between the parties, regardless of the form or medium through which it is facilitated (Satria et al., 2025).

In electronic transactions, particularly e-commerce, contracts are almost invariably standard contracts. These clauses are unilaterally designed by businesses or platforms and presented without any room for negotiation, leaving consumers with only the option to "accept or reject" without the ability to modify the content. This phenomenon reflects an imbalance in bargaining power between commercially dominant business actors and relatively vulnerable consumers in digital contractual relationships — a condition that has become a real and recurring source of problems in modern consumer protection (Sina, Ubay, & Nur Saputra, 2026). In the context of electronic transactions, agreements are transmitted through a cyber-network structure and have received normative legitimacy through Law Number 11 of 2008, subsequently refined by Law Number 1 of 2024 concerning Information and Electronic Transactions (the ITE Law) (Nugraha, 2021). The validity of online agreements is explicitly and imperatively regulated in Article 18, paragraph (1) of the ITE Law, which provides that electronic transactions embodied in electronic contracts are binding upon the parties concerned (Kakisina et al., 2023).

This provision embodies the adoption of the principle of functional equivalence, a crucial doctrine originating from the UNCITRAL Model Law on Electronic Commerce. This principle establishes that an electronic document, data message, or digital identity must be treated on equal footing with a conventional written document, to the extent that the basic functions of the instrument are fulfilled — namely, identifying the transacting party, recording the trail of consent, and ensuring that the integrity of the information can be conclusively verified and accessed for future reference (Kakisina et al., 2023). Through the lens of doctrinal law, the application of the functional equivalence principle removes the dogmatic disadvantage attached to binary code strings in cyberspace, transforming them into legal instruments subject to the principle of *pacta sunt servanda* as enshrined in Article 1338 of the Civil Code.

However, a prescriptive analysis reveals that the ITE Law, within the framework of contract law, operates only as a *lex specialis* regulating the medium of transmission, while the essential parameters of contractual validity remain absolutely governed by the *lex generalis*, namely Article 1320 of the Civil Code (Nugraha, 2021). Electronic contracts do not constitute a new species of law immune from general contractual validity requirements. A digital agreement can therefore only be qualified as valid and enforceable if it cumulatively satisfies the four pillars of contractual validity: consensus, legal capacity, a determinate object, and a

lawful cause. This harmonious integration of modern technological instruments with classical legal doctrine confirms that the technological medium merely facilitates the transmission of will, while the legality of the act itself must be assessed through the dogmatic instruments of civil law.

In addressing the fulfillment of the requirements for contractual validity, this study identifies a sharp conceptual conflict between the concept of legal capacity under the conventional civil law system and the uncertainty inherent in electronic transactions. Article 1330 of the Civil Code draws a strict boundary by classifying minors as legally incapable of performing legal acts, including entering into agreements. The rationale for this restriction is to protect minors' interests from impulsive decisions, given their presumed lack of the cognitive and psychological maturity required to appreciate the civil consequences of their actions.

However, the transition to a digital commercial ecosystem is eroding this protective framework. Neither the ITE Law nor the Government Regulation on the Implementation of Electronic Systems and Transactions provides a specific preventive mechanism or establishes a clear age threshold for determining who has legal standing to express digital consent. Article 2 of the ITE Law broadly provides that the Law applies to every person who performs a legal act — a formulation that indirectly expands participation without imposing strict age filters.

The absence of a comprehensive Know Your Customer (KYC) identity verification layer on marketplace, online gaming, and e-commerce platforms has enabled minors to actively participate as parties to online agreements. Empirical evidence reveals the widespread occurrence of virtual item purchases, microtransactions, and subscriptions to paid digital services carried out unilaterally by children without parental or guardian consent or supervision.

From the perspective of contract law doctrine, the failure to satisfy the capacity requirement does not render the contract void *ab initio*. Rather, under civil law, the requirements of consensus and capacity are classified as subjective conditions, the non-fulfillment of which renders the agreement voidable rather than null and void (*nietig van rechtswege*) (Miru & Pati, 2014). This means that an electronic contract concluded by a minor is born with a legal defect but remains binding until a request for annulment is filed by an interested party — the parent or guardian — before a court of first instance (Suparni, 2009).

This legal construction creates a dual vulnerability within the digital economy. Compliant electronic businesses are exposed to substantial commercial risk, as products, services, or digital assets already transferred may be nullified at any time on grounds of the consumer's subjective incapacity (August, 2020). Conversely, the relaxation of age verification requirements creates an exploitable loophole for technology companies that can readily monetize the uninformed consent of minors. This study therefore emphasizes that weaknesses in authentication in electronic contracts strike at the very core of the requirement of free and rational will. A fundamental legal reform is required to compel smart contract operators and online trading platforms to integrate biometric age authentication systems or real-time synchronization with digital population identity data, in order to neutralize the risk of electronic contract annulment arising from the absence of legal capacity.

The analysis further extends to the distortion of consensual validity in online agreements. In the conventional legal order, ideal consensualism is born of an equal and deliberative bargaining process between the parties. This paradigm is dissolving in the digital ecosystem,

where most electronic agreements are concluded through standard contract schemes in the form of clickwrap or browsewrap mechanisms (Prince, Catholic, & Cendika, 2014). Users are typically confronted with a single digital interface presenting terms and conditions drafted in complex legal language, concluded by a single-choice mechanism that presupposes unanimous consent (Debora et al., 2024).

The use of standard contracts in this manner materially undermines the principle of freedom of contract, reducing it in practice to the mere freedom to acquiesce to corporate dictates. This power imbalance is further aggravated by the common practice of embedding exoneration clauses — provisions designed to eliminate, divert, or limit the liability of business actors for product defects, service failures, and consumer data breaches — in a manner that renders them inconspicuous to consumers (Pohan, Priowirjanto, & Ramli, 2023).

In response to this phenomenon, Article 18, paragraph (1) of Law Number 8 of 1999 concerning Consumer Protection (UUPK) must be more rigorously enforced. This provision expressly prohibits the inclusion of exoneration clauses, and any agreement containing such clauses is subject to nullity (*nietig van rechtswege*), meaning that the exemption clause is deemed never to have existed and carries no binding force under civil law.

Notwithstanding these protections, the harmonization of Indonesian legislation in this domain remains incomplete. The ITE Law does not contain specific provisions governing the limitations and legal boundaries on the use of standard clauses in cyberspace, leaving consumers subject to exclusive choice-of-law provisions or cross-jurisdictional arbitration forums that significantly disadvantage their bargaining position (Debora et al., 2024). As a consequence of this regulatory inconsistency, an electronic contract that formally appears valid by virtue of a clickwrap signature may lose its material legitimacy where its substance is defective, contains a prohibited cause, or violates public order. This confirms the juridical proposition that formal legitimacy does not necessarily produce substantive justice, particularly when the legal system permits consent to be systematically extracted through the architecture of a digital interface.

## **H.2. The Evidentiary Power of Digital Evidence in the Dynamics of Civil Dispute Resolution**

This study examines questions regarding the evidentiary weight of digital evidence in the contemporary era before proceeding to an analysis of the formal legal system. In Indonesia, civil procedure law has historically been designed to resolve disputes in the physical, paper-based domain. The *Herzien Inlandsch Reglement (HIR)* and the *Rechtsreglement Buitengewesten (RBg)* provide the operational foundation, recognizing five conventional instruments of proof: written documents, witness testimony, presumptions, confessions, and oaths.

With the advent of the modern digital era, mobile devices, emails, server logs, and instant messaging screenshots have become the primary channels of human interaction, creating a normative gap in relation to conventional evidentiary sources. Article 5, paragraphs (1) and (2) of the ITE Law have amended the national civil procedure framework by explicitly stipulating that electronic information, electronic documents, and their printed outputs constitute valid evidence under Indonesian procedural law (Syamsulbahri, 2023). This places electronic evidence on a par with conventional proof, carrying formal, material, and elemental evidentiary

value, provided that the electronic security procedures cannot be successfully challenged by the opposing party in court.

This normative recognition, however, has encountered practical obstacles. Judicial institutions face significant challenges because digital data is inherently volatile, mediated by complex algorithms, lacks a stable physical form, and is highly susceptible to manipulation through techniques such as deepfakes, destruction of binary structures, and metadata alteration. The evolution of the Indonesian judiciary through the implementation of electronic court administration and proceedings (e-Court), legitimized by Supreme Court Regulation (Peraturan Mahkamah Agung/PERMA) Number 3 of 2018 and PERMA Number 1 of 2019, has promised greater efficiency and transparency in the resolution of civil disputes (Miftakur Rohman, 2022). With the digitization of court proceedings — encompassing the submission of electronic files, electronic hearing summonses, written pleadings, and the submission of evidence through the court's information technology system — the bench must apply rigorous standards to distinguish digital evidence from official and physical evidence (Amelia et al., 2021).

This study analyzes formal validity (procedural validity), defined as the capacity of an electronic document to satisfy the administrative and technical requirements for legal validity in accordance with civil procedural rules. An agreement in Portable Document Format (PDF) or a record of transaction activity must allow traceability of its metadata and transmission source, or be protected by an asymmetric digital signature guaranteeing irrefutable authenticity from the moment of signing through to its submission to the court clerk (Bachsin et al., 2025). Where a party fails to satisfy these formal requirements, the evidence is considered inadmissible on grounds of procedural invalidity.

Material validity, also referred to as substantive truth, focuses on the content, value, integrity, and factual accuracy conveyed by an electronic document. This assessment examines whether the recorded data is authentic and has not been altered through software manipulation, artificial editing, or other forms of distortion. Material validity invariably requires a scientific approach, including computational trail audits, cyber forensic verification, data authenticity analysis, and expert IT witness testimony — methods necessitated by the fact that digital data cannot be assessed with the naked eye as conventional wet signatures and scanned documents can. These forensic methods serve as validation tools to confirm that a file submitted to the e-Court system retains the same binary structure as it had at the time the legal event occurred.

Where material validity standards are not met, an electronic document submitted to the e-Court system loses its probative value. It can no longer serve as conclusive evidence capable of exonerating a party; instead, it is treated as an indication, preliminary evidence, or a presumption subject to judicial discretion in determining the underlying facts (Bachsin et al., 2025).

This research also conducts a practical review of jurisprudence and court decisions as instruments of law formation. Supreme Court Decision No. 300K/Pdt/2010 in the well-known case of Prita Mulyasari constitutes a significant legal milestone in the development of Indonesian law concerning the evidentiary validity of electronic mail. In its legal reasoning, the Supreme Court unequivocally affirmed that emails may be lawfully downloaded and printed from a service provider's system dashboard, provided that basic authentication parameters have been satisfied and the opposing party presents no concrete evidence of data

manipulation. This precedent reinforces the application of the principle of functional equivalence in judicial proceedings.

However, consistency in jurisprudence at the cassation level appears to be undermined by divergence and inconsistency at the district court and appellate court levels, giving rise to a crisis of legal certainty. In one jurisdiction, the Central Jakarta District Court (Decision No. 1234/Pdt.G/2022/PN.Jkt.Pst) accepted screenshots of WhatsApp messages as valid documentary evidence. By contrast, comparable evidence was rejected outright by the Surabaya District Court (Decision No. 876/Pdt.G/2023/PN.Sby) (Utami & Wiraguna, 2025). The rejection was grounded in a normative-conservative position that two-dimensional printed evidence is deficient because it does not satisfy the formal proof requirements of the HIR's legacy evidentiary system, and more specifically because no computational forensic examination had been conducted on the original physical mobile device (hardware) storing the data (Pradipa & Ganesha, 2025).

This divergence in judicial reasoning supports the central hypothesis of this research: where the dynamics of law rest solely on judicial discretion without strict, measurable, and parametric formal legal rules governing intangible evidence, the legal system risks producing outcomes akin to a speculative adjudicatory process. The legal uncertainty that undermines equality before the law for litigants may ultimately be attributed to unconstrained judicial discretion in interpreting the credibility of digital transaction log evidence.

### **H.3. Technical and Juridical Obstacles in Digital Proof Based on the Law**

To address the identified obstacles, this analysis examines the findings thoroughly. The results indicate that, although Article 5 of the ITE Law is declarative in nature, the transition from paper-based justice to a digitally adaptive judiciary has not been seamless. A tension exists between legal barriers — procedural gaps — and technical barriers — institutional technological deficiencies — giving rise to epistemological conflicts at the foundations of legal institutions (Islam & Sumatra, 2024).

The analysis reveals a structural inconsistency within the formal legal framework: the visionary substantive provisions of the ITE Law are not supported by a corresponding reform of national civil procedure law, which remains outdated and anchored in colonial-era texts from the Dutch East Indies period (the HIR and RBg). Law enforcement agencies have yet to formulate technical verification procedures for electronic evidence.

First, a dangerous interpretive gap arises from the absence of a legally regulated standard operating procedure (SOP) governing the submission, cross-examination, and validation of digital evidence. No clear standard exists for transferring files to a court computer without causing interference that could compromise the binary structure of the data, with the consequence that electronic contract evidence may lose its material probative value (Pradipa & Ganesha, 2025).

Second, the burden of proof system in cyber civil disputes has generated considerable controversy regarding its proper allocation. This system is premised on the classical principle of Article 163 of the HIR, which provides that whoever asserts a right bears the obligation to prove it. In the context of e-commerce, however, this creates a pronounced imbalance: individual consumers lack administrative access — commonly referred to as backend privilege — to large corporate database servers, and are therefore unable to produce authentic digital

evidence. The principle of equality of arms is undermined by the failure to adequately accommodate a doctrine of reversal of the burden of proof within the ITE Law, effectively silencing consumer voices before proceedings have begun.

At the operational and governance level, the key findings of this research suggest that the modernization of courts through the integrated e-Court application addresses only the surface-level administrative functions — such as electronic payments, registration tracking, and electronic hearing summonses — without resolving the core challenges of digitizing the evidentiary process (Amelia et al., 2021).

The high costs involved, compounded by the country's lack of adequate digital forensic laboratories to support civil litigation, pose significant obstacles. Tracing the origins of smart contract algorithms, detecting steganography in PDF files, or verifying the hash functions of fraudulent signatures requires specialized software that is prohibitively expensive for litigants required to engage expert IT witnesses (Syamsulbahri, 2023).

Furthermore, the digital literacy deficit affecting members of the judiciary and legal practitioners constitutes a particularly serious risk factor. Field evidence indicates that the traditional mindset of legal practitioners exhibits a dogmatic resistance to validating evidence without physically handling stamped documents. Judges accustomed solely to textual analysis are unlikely to be familiar with reading source code, interpreting Penyelenggara Sertifikasi Elektronik (PSrE) electronic certificates, or understanding blockchain logic. This intellectual reluctance to engage with technological innovation ultimately undermines the principles of the ITE Law, threatens consumer protection, and erodes legal certainty.

Given the multi-layered complexity of the conflict between dogmatic approaches to the validity of digital contracts and the procedural disruptions associated with electronic evidence, the overarching conclusions of this study set out a prescriptive solution grounded in a policy reform framework.

### **H.3.1. Integration of Population System Interoperability as a Verifier of Eligibility Requirements**

The state must enforce technical compliance regulations through the Ministry of Communication and Information, in collaboration with the Directorate General of Population and Civil Registration. This regulation requires large-scale e-commerce platforms to integrate application programming interfaces with a centralized biometric National Identity Number (NIK) system (Saputri, 2024). This advanced age filter will prevent vulnerable transactions from being canceled, protecting children from exploitative contracts, and preventing business losses for online sellers.

### **H.3.2. Deconstructing Standard Clauses in Virtual Space**

The government is urged to establish a cyber legal framework by issuing regulations at the level of Government Regulation in accordance with Article 18 of the Electronic Transactions Law for digital platforms. To obtain an exemption from liability or an arbitration option, this business ecosystem must implement a multi-layered consent mechanism, or open consent. In long, hard-to-read text or with a single agree button.

### **H.3.3. Formal Reform of Supreme Court Procedures Related to Electronic Evidence**

Gaps in civil procedure standards must be addressed immediately. The Supreme Court must issue the Supreme Court Regulation (PERMA) on Digital Evidence Audit Standards explicitly and comprehensively after the completion of the Draft Code of Civil Procedure.

(Pradipa and Ganesha 2025) The PERMA should govern the digital storage network scenario, define criteria for distinguishing PSrE-signed documents from mere mechanical printouts, and institute server discovery commands for information stored on the server.

#### **H.3.4. Judicial Forensic Development and Improvement of Legal Literacy**

The establishment of the Supreme Court's Electronic Forensics Center is critical to addressing the gap in IT expertise in the judiciary. Eventually, this judicial laboratory will serve all courts across the country. Cyber agreement analysis, asymmetric encryption, and telematics law should be incorporated into large-scale judicial education programs. It is expected that this eclectic alignment between judicial, dogmatic, and technological elements will remove the clarity from the uncertainty in the world of online agreements, restoring the dignity and robustness of Indonesia's legal architecture to align with the progress of interactive civilization in the 21st century.

### **CONCLUSION**

The shift of the transaction medium to cyberspace does not extinguish the foundations of classical contract doctrine but merely positions the ITE Law as a *lex specialis* governing the technological medium alone. The essential conditions for the validity of a contract remain anchored to the pillars of Article 1320 of the Civil Code. Practice in the field reveals inherent defects in digital agreement instruments, ranging from the absence of demographic filters that allow minors to freely bind themselves — thereby giving rise to voidable agreements — to covert manipulation through standard contracts in clickwrap format. The practice of corporations unilaterally embedding exoneration clauses suppresses the principle of freedom of contract and renders such clauses potentially null and void by operation of law, as they conflict with consumer protection provisions. Moving to the realm of formal law, the recognition of electronic data as valid legal evidence has not been accompanied by commensurate readiness in judicial infrastructure or human resources. When digital documents become the subject of e-Court disputes, the bench is confronted with a proof dilemma arising from the volatile and highly manipulable character of binary data. The absence of standard operating procedures (SOPs) governing technical verification and the lack of forensic audit guidelines have created a gap that produces inconsistency in decisions across court levels. As a result, the formal validity of electronic evidence is frequently denied simply because judges encounter difficulty in testing its material validity — a predicament compounded by the low technological literacy of law enforcement officials and the prohibitive cost of engaging forensic experts for ordinary litigants.

### **REFERENCES**

- Amelia, A. A. (2021). Sistem e-court dalam pelaksanaan peradilan di Indonesia pada masa pandemi COVID-19. *6*(2), 125–143.
- Bachsin, A., Fathi, H., Ekoputro, H., Ikram, H., & Ranggana, A. (2025). Kedudukan dan penilaian hakim terhadap alat bukti elektronik dalam proses pembuktian perkara perdata. *Al-Zayn: Jurnal Ilmu Sosial & Hukum*, *3*(3), 2364–2370.
- Bernstein, L. (2015). Beyond relational contracts: Social capital and network governance in procurement contracts. *Journal of Legal Analysis*, *7*(2), 561–621.
- Debora, C., Stefani, G. C., Haezer, E., & Putrayasa, W. (2024). Implikasi yuridis klausula baku perjanjian elektronik dalam transaksi di e-commerce. *Jurnal Ilmu Sosial dan*

- Humaniora*, 8, 146–153. [Jurnal Kultura](#)
- Islam, U., & Negeri Sumatera. (2024). Analisis kritik pembuktian elektronik dalam hukum acara perdata: Tantangan dan prospek di Indonesia. *5*(2), 39–47.
- Kakisina, P. H., Gosal, V. Y., & Nachrawy, N. (2023). Keabsahan kekuatan pembuktian kontrak elektronik dalam perjanjian bisnis menurut hukum positif di Indonesia. *11*(4).
- Miftakur Rohman, A. K. (2022). Implementasi e-court terhadap pelayanan administrasi perkara di Pengadilan Agama Gresik. *2*(April), 324–342.
- Miru, A., & Pati, S. (2014). *Hukum perikatan: Penjelasan makna Pasal 1233 sampai 1456 BW* (6th ed.). Rajawali Pers.
- Nugraha, S. N. (2021). Cidera janji (wanprestasi) dalam perjanjian fidusia berdasarkan Pasal 15 ayat (3) UU Nomor 42 Tahun 1999 pasca putusan Mahkamah Konstitusi Nomor 18/PUU-XVII/2019. *Al Wasath Jurnal Ilmu Hukum*, *2*(2), 77–92. <https://doi.org/10.47776/alwasath.v2i2.213>
- Pohan, T. G., Priowirjanto, E. S., & Ramli, T. S. (2023). Analisis penggunaan perjanjian baku elektronik berklauseksonerasi pada marketplace ditinjau berdasarkan hukum positif Indonesia. *COMSERVA: Jurnal Penelitian dan Pengabdian Masyarakat*, *3*(7), 2913–2924. <https://doi.org/10.59141/comserva.v3i07.1075>
- Pradipa, A. (2025). Analisis terhadap kedudukan alat bukti elektronik dalam pembuktian perkara perdata pasca UU ITE dan perkembangan e-court. Universitas Pendidikan Ganesha.
- Savelyev, A. (2017). Contract law 2.0: Smart contracts as the beginning of the end of classic contract law. *Information & Communications Technology Law*, *26*(2), 116–134.
- Satria, R., Yuliastini, A., Sebayang, A., Wagner, I., & Fitriani, Y. (2025). Keabsahan perjanjian digital dalam transaksi elektronik berdasarkan Undang-Undang Informasi dan Transaksi Elektronik. *Jurnal Kolaboratif Sains*, *8*(1), 557–567. <https://doi.org/10.56338/jks.v8i1.6708>
- Sina, I., Ubay, H., & Saputra, R. N. (2026). Tanggung jawab hukum marketplace dalam pembelian online dan transaksi jual beli di Indonesia: Analisis efektivitas perlindungan konsumen digital. *Legisici*, *3*(4), 340–366. <https://doi.org/10.62885/legisici.v3i4.1058>
- Soekanto, S. (1986). *Pengantar penelitian hukum*. UI Press.
- Soekanto, S., & Sri, M. (2007). *Penelitian hukum normatif*. Rajawali Pers.
- Suparni, N. (2009). *Cyberspace: Problematika dan antisipasi pengaturannya* (Cet. 1). Mizan Pustaka.
- Sutrisno, E., Kartina, R. M., Rahman, A., Sanusi, & Dikrurahman, D. (2021). *Pedoman penulisan skripsi*. Deepublish.
- Syamsulbahri, H. (2023). Eksistensi alat bukti elektronik pada pembuktian perkara perdata. *Jurnal Pengadilan Tinggi Agama Jakarta*, *12*, 1–58.
- Usman, T. (2020). Keabsahan tanda tangan elektronik pada perjanjian jual beli barang dari perspektif hukum perdata. *Indonesia Private Law Review*, *1*(2), 87–98. <https://doi.org/10.25041/iplr.v1i2.2058>
- Utami, G. C., & Wiraguna, S. A. (2025). Pembuktian digital dalam sengketa perdata: Menguji validitas formil dan materiil dokumen elektronik di era modern. *2*(November), 40–52.